**Buffer overflow**

**Traccia:**

Abbiamo già parlato del buffer overflow, una vulnerabilità che è conseguenza di una mancanza di controllo dei limiti dei buffer che accettano input utente. Nelle prossime slide vedremo un esempio di codice in C volutamente vulnerabile ai BOF, e come scatenare una situazione di errore particolare chiamata «segmentation fault», ovvero un errore di memoria che si presenta quando un programma cerca inavvertitamente di scrivere su una posizione di memoria dove non gli è permesso scrivere (come può essere ad esempio una posizione di memoria dedicata a funzioni del sistema operativo).

**Esecuzione:**

Il buffer overflow, o sovraccarico di buffer, è un problema di sicurezza che si verifica quando un programma scrive più dati di quelli che può contenere un buffer allocato nella memoria del computer.

Nel caso di un buffer overflow, il programma, per vari motivi, tenta di inserire più dati di quanti ne possa effettivamente contenere il buffer. Questo può sovrascrivere dati o codice nelle aree di memoria adiacenti.

A screenshot of a computer

Description automatically generated

Questo è il programma che abbiamo scritto che va a richiedere un nome di massimo di 10 caratteri, la consegna ci dice di portare questo valore a 30 caratteri.

A screenshot of a computer program

Description automatically generated

Se inseriamo più di 30 caratteri il programma ci ritorna un errore, «segmentation fault», ovvero errore di segmentazione. L’errore di segmentazione avviene quando un programma, come abbiamo detto in precedenza, tenta di scrivere contenuti su una porzione di memoria alla quale non ha accesso. Questo è un chiaro esempio di BOF.